



## On a Theorem of Göbel on Permutation Invariants

Müfit Sezer

To cite this article: Müfit Sezer (2008) On a Theorem of Göbel on Permutation Invariants, Communications in Algebra, 36:10, 3723-3729, DOI: [10.1080/00927870802158051](https://doi.org/10.1080/00927870802158051)

To link to this article: <http://dx.doi.org/10.1080/00927870802158051>



Published online: 28 Oct 2008.



Submit your article to this journal [↗](#)



Article views: 46



View related articles [↗](#)

## ON A THEOREM OF GÖBEL ON PERMUTATION INVARIANTS

Müfit Sezer

Department of Mathematics, Bilkent University, Ankara, Turkey

*Let  $F$  be a field, let  $S = F[X_1, \dots, X_n]$  be a polynomial ring on variables  $X_1, \dots, X_n$ , and let  $G$  be a group of permutations of  $\{X_1, \dots, X_n\}$ . Göbel proved that for  $n \geq 3$  the ring of invariants  $S^G$  is generated by homogeneous elements of degree at most  $\binom{n}{2}$ . In this article, we obtain reductions in the set of generators introduced by Göbel and sharpen his bound for almost all permutation groups over any ground field.*

**Key Words:** Permutation groups; Polynomial invariants.

**2000 Mathematics Subject Classification:** 13A50.

### INTRODUCTION

In this article,  $V$  denotes a finite dimensional vector space over a field  $F$ , on which a finite group  $G$  acts faithfully from the left. The action of  $G$  on  $V$  extends to an action on the symmetric algebra  $S = S_F(V)$ . For  $f \in S$  and  $g \in G$ , we let  $g(f)$  denote the image of  $f$  under  $g$ . We study the algebra of invariant polynomials

$$S^G = \{f \in S \mid g(f) = f \text{ for all } g \in G\}.$$

This is a graded subalgebra of  $S$ . By a famous theorem of E. Noether (1926),  $S^G$  is finitely generated. Let  $\beta(G, V)$  denote the smallest integer  $d$  such that  $S^G$  is generated by elements of degree at most  $d$ . A classical problem is to obtain upper bounds for  $\beta(G, V)$ . We refer the reader to two recent surveys by Neusel (2007) and Wehlau (2006) for an overview of known results on this problem.

Here we study the situation where  $G$  is a subgroup of the symmetric group  $\mathfrak{S}_n$  acting naturally on a basis  $X_1, \dots, X_n$  of  $V$  by  $\sigma(X_i) = X_{\sigma(i)}$  for  $\sigma \in G$ . In this case, we identify  $S$  with the polynomial ring  $F[X_1, \dots, X_n]$  in the variables  $X_1, \dots, X_n$ . By constructing a specific set of generators, Göbel (1995) proves that for  $n \geq 3$  the ring of invariants  $S^G$  is generated by homogeneous elements of degree at most  $\binom{n}{2}$ . Every minimal set of algebra generators for the invariants of the alternating group  $A_n$  contains an element of degree  $\binom{n}{2}$ , so his bound is best possible in general.

Received February 24, 2007; Revised July 26, 2007. Communicated by T. H. Lenagan.

Address correspondence to Müfit Sezer, Department of Mathematics, Bilkent University, Ankara 06800, Turkey; Fax: +90-312-2664579; E-mail: sezer@fen.bilkent.edu.tr

In this article, we obtain further reductions of the set of generators introduced by Göbel (see Remark 3). Consequently, we decompose the invariant polynomials of degree  $\binom{n}{2}$  for every permutation group except for  $A_n$  and four other groups.

**Theorem 1.** Assume that  $n > 3$ . If  $G$  is a permutation group such that  $\beta(G, V) = \binom{n}{2}$ , then  $G = A_n$  or  $G$  is isomorphic to one of the following four groups:

1.  $n = 5$  and  $A_1(5)$ ;
2.  $n = 6$  and  $PGL_2(5)$ ;
3.  $n = 9$  and  $PGL_2(8)$ ;
4.  $n = 9$  and  $P\Gamma L_2(8)$ ;

where  $A_1(q)$  is the affine group on the  $q$  points of the line over the field of  $q$  elements,  $PGL_2(q)$  and  $P\Gamma L_2(q)$  are the groups of all linear and semilinear transformations of the projective line over the field with  $q$  elements, respectively.

As a general reference for the invariant theory of finite groups, we recommend Derksen and Kemper (2002) and Neusel and Smith (2002).

## 1. MAIN REDUCTIONS

We let  $M$  denote the set of monomials in the variables  $X_1, \dots, X_n$ . We use the symbol  $<$  to denote the lexicographic order on  $M$  with  $X_1 > X_2 > \dots > X_n$ . Given a polynomial  $f = \sum a_{e_1, \dots, e_n} X_1^{e_1} \dots X_n^{e_n}$ , we say that a monomial  $X_1^{e_1} \dots X_n^{e_n}$  appears in  $f$ , or is in  $f$ , if  $a_{e_1, \dots, e_n} \neq 0$ . Let  $G_m$  denote the stabilizer of a monomial  $m$  and let

$$o(m) = \sum_{\tilde{h} \in G/G_m} h(m)$$

denote the orbit sum of  $m$ . It is easy to see, and it is well known, that the orbit sums of monomials form a  $F$ -linear basis for  $S^G$ .

As in Göbel (1995), a monomial  $m = X_1^{e_1} \dots X_n^{e_n}$  is called *special* if either  $\{e_1, \dots, e_n\}$  contains all integers in the set  $\{0, 1, \dots, \max\{e_1, \dots, e_n\}\}$ , or  $e_1 = \dots = e_n = 1$ . For each  $m \in M$ , there exists a permutation  $\pi \in \mathfrak{S}_n$  such that  $\pi(m) = X_1^{e_1} \dots X_n^{e_n}$  satisfies  $e_1 \geq e_2 \geq \dots \geq e_n$ . The monomial  $\pi(m)$  is called the *descending form* of  $m$  and is denoted  $\text{desc}(m)$ . We say that  $m$  is descending if  $m = \text{desc}(m)$ .

An orbit sum  $o(m)$  is called *expressible* if it is contained in the  $F$ -algebra generated by orbit sums of monomials that have strictly smaller degree or strictly smaller descending form. We use the following result, due to Göbel (1995). It is taken from theorem (Göbel, 1995, 3.11) and its proof.

**Göbel's Theorem.** The orbit sum  $o(m)$  of every nonspecial monomial  $m$  is contained in the subalgebra generated by the orbit sums  $o(m')$  of special monomials  $m'$  with  $\text{desc}(m') < \text{desc}(m)$ . In particular, if  $n \geq 3$ , then  $S^G$  is generated by invariant polynomials of degree at most  $\binom{n}{2}$ .

If  $a, b$  are integers with  $a \leq b$ , then  $[a, b]$  denotes the set  $\{i \in \mathbf{Z} \mid a \leq i \leq b\}$ . Let  $m = X_1^{e_1} \dots X_n^{e_n}$  be a monomial. For each integer  $j$ , we set

$$\text{supp}_j(m) = \{i \in [1, n] \mid e_i = j\};$$

$$\text{supp}_{\geq j}(m) = \{i \in [1, n] \mid e_i \geq j\}.$$

**Remark 1.** If  $m$  and  $m'$  are monomials in  $M$ , then the followings hold.

1.  $\text{desc}(h(m)) = \text{desc}(m)$  for all  $h \in \mathfrak{S}_n$ ;
2.  $\text{desc}(m) = \text{desc}(m')$  if and only if  $|\text{supp}_j(m)| = |\text{supp}_j(m')|$  for all  $j \geq 0$ ;
3.  $\text{desc}(m) \succ \text{desc}(m')$  if and only if there exists an integer  $r$  such that

$$\begin{aligned} |\text{supp}_r(m)| &> |\text{supp}_r(m')|; \\ |\text{supp}_j(m)| &= |\text{supp}_j(m')| \quad \text{for all } j > r. \end{aligned}$$

The properties listed above follow easily from the definitions.

To every monomial  $m \in M$  and every  $j \in [1, n]$  we associate the monomials

$$m_j = \prod_{i \in \text{supp}_{\geq j}(m)} X_i \quad \text{and} \quad \tilde{m}_j = \frac{m}{m_j}$$

and the invariant polynomial

$$P_{m,j} = o(\tilde{m}_j) \cdot o(m_j). \quad (1)$$

It is easy to see that the polynomial  $P_{m,j}$  satisfies the equality:

$$P_{m,j} = \sum_{\tilde{h} \in G/G_{\tilde{m}_j}} h(\tilde{m}_j \cdot o(m_j)). \quad (2)$$

The central step in the proof of Göbel's Theorem (1995, 3.11) is to express an orbit sum of a *nonspecial* monomial in terms of orbit sums of monomials that have strictly smaller descending form. To obtain a sharpening of Göbel's bound we analyze the decomposition of orbit sums of special monomials.

The following lemma is our main reduction result. We show that Göbel's decomposition applied to the orbit sum of a special monomial  $m$  nevertheless contains only the monomials that have the same or strictly smaller descending forms. It is the appearance of different orbit sums of monomials with the same descending form as  $m$  in this decomposition that prevents the orbit sum of  $m$  from being expressible. We examine such orbit sums in the lemma and collect the group elements required so that these orbit sums appear in the decomposition.

**Lemma 2.** Let  $m$  be a monomial,  $j$  a positive integer,  $g$  an element of  $G$ , and set

$$t = \tilde{m}_j \cdot g(m_j).$$

The following then hold:

1.  $\text{desc}(t) \leq \text{desc}(m)$ . More precisely

$$\begin{aligned} \text{desc}(t) &= \text{desc}(m) && \text{if } \text{supp}_{\geq j+1}(m) \subseteq g(\text{supp}_{\geq j}(m)) \subseteq \text{supp}_{\geq j-1}(m); \\ \text{desc}(t) &< \text{desc}(m) && \text{otherwise.} \end{aligned}$$

In particular, all monomials that appear in  $P_{m,j}$  have smaller or equal descending forms than that of  $m$ .

2. If  $\text{desc}(t) = \text{desc}(m)$ , then

$$\begin{aligned}\text{supp}_r(t) &= \text{supp}_r(m) \quad \text{for } r \neq j, j-1; \\ \text{supp}_{\geq j}(t) &= g(\text{supp}_{\geq j}(m)).\end{aligned}$$

3. The monomial  $m$  appears in  $P_{m,j}$  with coefficient one.

4. If  $o(m)$  is not expressible and  $m_j \neq 1$ , then there exists an element  $h \in G$  such that the monomial  $u = \tilde{m}_j \cdot h(m_j)$  has the following properties:  $\text{desc}(u) = \text{desc}(m)$ , the monomial  $u$  does not appear in  $o(m)$ , and  $o(u)$  is not expressible.

*Proof.* 1. and 2.

We may assume that  $m$  is descending by Remark 1. Furthermore since the assertions hold trivially for  $t = m$ , we may take  $g(m_j) \neq m_j$  so that  $m \neq t$ . Notice that  $g(m_j) \neq m_j$  if and only if  $g(\text{supp}_{\geq j}(m)) \neq \text{supp}_{\geq j}(m)$ . In particular, we assume that  $[1, n] \setminus g(\text{supp}_{\geq j}(m)) \neq \emptyset$ .

Let  $i$  denote the smallest number in  $[1, n] \setminus g(\text{supp}_{\geq j}(m))$  and let  $s$  denote the largest number in  $g(\text{supp}_{\geq j}(m))$ . Since  $g(\text{supp}_{\geq j}(m)) \neq \text{supp}_{\geq j}(m)$  and  $m$  is descending, it follows that  $i \in \text{supp}_{\geq j}(m)$  and  $s \notin \text{supp}_{\geq j}(m)$ . Hence  $e_i \geq j$  and  $e_s \leq j-1$ . Furthermore,  $e_i = j$  if and only if  $\text{supp}_{\geq j+1}(m) \subseteq g(\text{supp}_{\geq j}(m))$ . We also have  $e_s = j-1$  if and only if  $g(\text{supp}_{\geq j}(m)) \subseteq \text{supp}_{\geq j-1}(m)$ . We now examine the different possibilities.

Assume first  $e_i > j$ . If  $d$  is in  $[1, i-1]$ , then  $X_d$  divides  $g(m_j)$ , so  $X_d^{e_d}$  divides  $t$ . It follows that  $\text{supp}_r(m) = \text{supp}_r(t)$  for  $r > e_i$ . On the other hand  $X_i^{e_i}$  does not divide  $t$ , so  $\text{supp}_{e_i}(m) \supsetneq \text{supp}_{e_i}(t)$ . Remark 1 now yields  $\text{desc}(m) \succ \text{desc}(t)$ .

Assume next for the rest of the proof that  $e_i = j$ . If  $d$  is in  $[1, i-1]$ , then  $X_d$  divides  $g(m_j)$ , so  $X_d^{e_d}$  divides  $t$ , hence  $\text{supp}_r(m) = \text{supp}_r(t)$  for  $r > e_i = j$ . Since  $\text{supp}_{\geq j+1}(m) \subseteq g(\text{supp}_{\geq j}(m))$ , we have

$$\begin{aligned}|g(\text{supp}_{\geq j}(m)) \setminus \text{supp}_{\geq j+1}(m)| &= |\text{supp}_j(m)| \quad \text{and} \\ \text{supp}_j(t) &= (g(\text{supp}_{\geq j}(m)) \setminus \text{supp}_{\geq j+1}(m)) \cap (\text{supp}_j(m) \cup \text{supp}_{j-1}(m)).\end{aligned}$$

If  $e_s < j-1$ , then  $s \in g(\text{supp}_{\geq j}(m)) \setminus \text{supp}_{\geq j+1}(m)$  but  $s \notin \text{supp}_j(m) \cup \text{supp}_{j-1}(m)$ . Therefore  $|\text{supp}_j(t)| < |g(\text{supp}_{\geq j}(m)) \setminus \text{supp}_{\geq j+1}(m)| = |\text{supp}_j(m)|$  and hence  $\text{desc}(m) \succ \text{desc}(t)$  by Remark 1.

If  $e_s = j-1$ , then  $\text{supp}_r(m) = \text{supp}_r(t)$  for all  $r < j-1$ , because  $X_d$  does not divide  $g(m_j)$  for all  $d$  with  $e_d < j-1$ . Moreover,  $e_s = j-1$  implies that  $(g(\text{supp}_{\geq j}(m)) \setminus \text{supp}_{\geq j+1}(m)) \subseteq (\text{supp}_j(m) \cup \text{supp}_{j-1}(m))$ . Hence  $\text{supp}_j(t) = g(\text{supp}_{\geq j}(m)) \setminus \text{supp}_{\geq j+1}(m)$  and therefore  $|\text{supp}_j(m)| = |\text{supp}_j(t)|$ . It follows from Remark 1 that  $\text{desc}(m) = \text{desc}(t)$ . We have also established  $\text{supp}_r(t) = \text{supp}_r(m)$  for  $r \neq j, j-1$  and  $\text{supp}_{\geq j}(t) = g(\text{supp}_{\geq j}(m))$ . Finally, since  $\text{desc}(t) \leq \text{desc}(m)$ , it follows  $\text{desc}(h(t)) \leq \text{desc}(m)$  for all  $h \in G$  by Remark 1. Therefore, all monomials that appear in  $P_{m,j}$  have smaller or equal descending forms than that of  $m$  in view of Eq. (2).

3. By a Mackey-formula for transfers (see Fleischmann, 1998, 2.1, 2.2), we have

$$P_{m,j} = o(\tilde{m}_j) \cdot o(m_j) = \sum_{h \in R} \frac{|G_{\tilde{m}_j \cdot h(m_j)}|}{|G_{\tilde{m}_j} \cap G_{m_j}^h|} o(\tilde{m}_j \cdot h(m_j)), \quad (3)$$

where  $G_{m_j}^h$  denotes  $hG_{m_j}h^{-1}$ , and  $R$  is a set of representatives of the  $G_{\tilde{m}_j} : G : G_{m_j}$  double cosets with  $1 \in R$ . If  $h = 1$ , then it is easy to see that  $|G_{\tilde{m}_j \cdot h(m_j)}| = |G_m| = |G_{\tilde{m}_j} \cap G_{m_j}|$ . Conversely, if  $o(\tilde{m}_j \cdot h(m_j)) = o(m)$ , then there is an element in  $G$ , say  $h'$ , such that  $\tilde{m}_j \cdot h(m_j) = h'(m)$ . We first want to prove that  $h' \in G_{\tilde{m}_j}$ . Note that  $\sigma \in \mathfrak{S}_n$  fixes a monomial  $u$  if and only if  $\text{supp}_i(u) = \sigma(\text{supp}_i(u))$  for all  $i$ . Applying part 2 with  $t = \tilde{m}_j \cdot h(m_j) = h'(m)$ , we see that  $\text{supp}_i(m) = \text{supp}_i h'(m) = h'(\text{supp}_i(m))$  for all  $i \neq j, j-1$ . Then it follows that  $\text{supp}_j(m) \cup \text{supp}_{j-1}(m)$  is also  $h'$ -stable since it is the complement in  $[1, n]$  of the union of the  $h'$ -stable sets  $\text{supp}_i(m)$  for  $i \neq j, j-1$ . Note that these  $h'$ -stable sets are precisely the “support” sets of  $\tilde{m}_j$ , namely  $\text{supp}_i(\tilde{m}_j) = \text{supp}_{i+1}(m)$  for  $i \geq j$ ,  $\text{supp}_{j-1}(\tilde{m}_j) = \text{supp}_j(m) \cup \text{supp}_{j-1}(m)$  and  $\text{supp}_i(\tilde{m}_j) = \text{supp}_i(m)$  for  $i \leq j-2$ . Therefore,  $h' \in G_{\tilde{m}_j}$ . From  $\tilde{m}_j \cdot h(m_j) = h'(m)$  it also follows that  $h(m_j) = h'(m_j)$ . Hence  $h \in G_{\tilde{m}_j} \cdot G_{m_j}$  and so  $h = 1$ . This proves that  $o(m)$  appears with multiplicity one in  $P_{m,j}$ .

4. By parts 1 and 3, if  $o(m)$  is not expressible, then there exists a monomial  $u$  in  $P_{m,j}$  with the same descending form as  $m$  such that  $o(u)$  is not expressible. Since  $P_{m,j}$  consists of orbit sums of the form  $o(\tilde{m}_j \cdot g(m_j))$  for  $g \in G$ , the assertion follows.  $\square$

In view of Eq. (3), we note a criteria for the redundancy of the orbit sum of a special monomial in the generating set as a consequence to the previous lemma.

**Remark 3.** Let  $R$  be a set of representatives of the  $G_{\tilde{m}_j} : G : G_{m_j}$  double cosets with  $1 \in R$ . Suppose  $m$  is a special monomial. Let  $G(m, j)$  denote the set of elements  $h \in R$  such that

$$\text{supp}_{\geq j+1}(m) \subseteq h(\text{supp}_{\geq j}(m)) \subseteq \text{supp}_{\geq j-1}(m) \quad \text{and} \quad \frac{|G_{\tilde{m}_j \cdot h(m_j)}|}{|G_{\tilde{m}_j} \cap G_{m_j}^h|} \neq 0 \in F.$$

Then  $o(m)$  is expressible if  $G(m, j) = \{1\}$  and  $m_j \neq 1$ .

## 2. DECOMPOSING ORBIT SUMS OF SPECIAL MONOMIALS OF DEGREE $\binom{n}{2}$

We first fix some notation. A group acting by permutations on a set  $P$  is said to be  $j$ -homogeneous for some natural number  $j$  if  $G$  acts transitively on the nonordered subsets of  $P$  of size  $j$ .

We say that a monomial  $m$  is *regular* if  $|\text{supp}_i(m)| = 1$  for  $i = 0, \dots, n-1$ . Note that for  $n > 3$ , special monomials of degree  $\binom{n}{2}$  are precisely the regular monomials. Let  $\sigma_i$  denote the transposition  $(i, i-1) \in \mathfrak{S}_n$ .

**Lemma 4.** *If there exists a regular monomial whose orbit sum is not expressible, then  $G$  is  $j$ -homogeneous for  $1 \leq j \leq n-1$ .*

*Proof.* Let  $m$  be such a special monomial. We start with the following observation.

**Claim.** The orbit sum of  $\sigma(m)$  is not expressible for all  $\sigma \in \mathfrak{S}_n$ .

Since every permutation in  $\mathfrak{S}_n$  is a product of transpositions  $\sigma_r$  with  $2 \leq r \leq n$ , it suffices to establish the claim for  $\sigma = \sigma_r$ . Without loss of generality, we may take  $m = X_1^{n-1} \cdot X_{n-1}^{n-2} \cdots X_2$ .

By Lemma 2, there exists  $g \in G$  such that  $\tilde{m}_{r-1} \cdot g(m_{r-1})$  does not lie in  $o(m)$  but has the same descending form as  $m$  and  $o(\tilde{m}_{r-1} \cdot g(m_{r-1}))$  is not expressible. We will show  $g(\text{supp}_{\geq r-1}(m)) = \text{supp}_{\geq r}(m) \cup \text{supp}_{r-2}(m)$  and that  $\tilde{m}_{r-1} \cdot g(m_{r-1}) = \sigma_r(m)$ . From Lemma 2, we have  $\text{supp}_{\geq r}(m) \subseteq g(\text{supp}_{\geq r-1}(m)) \subseteq \text{supp}_{\geq r-2}(m)$ , but  $\text{supp}_{\geq r}(m) = [r+1, n]$  and  $\text{supp}_{\geq r-2}(m) = [r-1, n]$ . It follows that  $g(\text{supp}_{\geq r-1}(m))$  is equal to either  $[r, n]$  or  $[r+1, n] \cup \{r-1\}$ . But if  $g(\text{supp}_{\geq r-1}(m)) = [r, n] = \text{supp}_{\geq r-1}(m)$ , then  $g(m_{r-1}) = m_{r-1}$ , and therefore  $\tilde{m}_{r-1} \cdot g(m_{r-1}) = m$ , which is a contradiction. Hence  $g(\text{supp}_{\geq r-1}(m)) = [r+1, n] \cup \{r-1\}$  and therefore  $\tilde{m}_{r-1} \cdot g(m_{r-1}) = \tilde{m}_{r-1} \cdot m_{r-1} \frac{X_{r-1}}{X_r} = \sigma_r(m)$  as desired. This establishes the claim.

Now let  $\sigma \in \mathfrak{S}_n$ . Since  $o(\sigma(m))$  is not expressible, the proof of the claim applied to  $\sigma(m)$  yields that there exists  $g \in G$  such that  $g(\text{supp}_{\geq r-1}(\sigma(m))) = \text{supp}_{\geq r}(\sigma(m)) \cup \text{supp}_{r-2}(\sigma(m))$ . Since  $\sigma$  is arbitrary, it follows that for an arbitrary pair of sets  $A = \text{supp}_{\geq r-1}(\sigma(m))$  of size  $n - r + 1$  and  $B = \text{supp}_{\geq r}(\sigma(m))$  of size  $n - r$  inside  $A$  and a point  $x = \text{supp}_{r-2}(\sigma(m))$  in  $[1, n] \setminus A$ , there exists  $g \in G$  such that  $g(A) = B \cup \{x\}$ . It follows that  $G$  is  $(n - r + 1)$ -homogeneous for  $2 \leq r \leq n$  as desired.  $\square$

**Proof of Theorem 1.** Since  $n > 3$ , a special monomial of degree  $\binom{n}{2}$  is a regular monomial. By Lemma 4, if  $G$  fails to be  $j$ -homogeneous for some  $j \in [1, n-1]$ , then the orbit sums of all regular monomials are expressible, forcing  $\beta(G, V) < \binom{n}{2}$ . By Beaumont and Peterson (1955, §11), if  $G$  is  $j$ -homogeneous for all  $j \in [1, n-1]$ , then  $G = \mathfrak{S}_n$ , or  $G = A_n$  or  $G$  is the one of the groups listed above. Since  $\beta(\mathfrak{S}_n, V) = n$ , the conclusion of the theorem follows.  $\square$

**Remark 5.** Note that we can make no claim as to the number  $\beta(G, V)$  if  $G$  is one of the four groups given in the statement of Theorem 1. Up to conjugation in  $\mathfrak{S}_n$ , these groups have the following generators given in Beaumont and Peterson (1955, §5):

1.  $A_1(5) = \langle (12345), (1325) \rangle \subseteq \mathfrak{S}_5$ ;
2.  $PGL_2(5) = \langle (12345), (12)(35), (13465), (1325) \rangle \subseteq \mathfrak{S}_6$ ;
3.  $PGL_2(8) = \langle (1254673), (15)(29)(47)(68) \rangle \subseteq \mathfrak{S}_9$ ;
4.  $PTL_2(8) = \langle (1254673), (15)(29)(47)(68), (124)(765) \rangle \subseteq \mathfrak{S}_9$ .

This information may be useful for direct computations of  $\beta(G, V)$  for these groups.

## ACKNOWLEDGMENT

The author thanks the anonymous referee for reading the article very carefully and valuable comments. In particular, the shorter and elegant proof of Lemma 2(3)

we present here is suggested to us by the referee. This improved proof also led to a sharpening of Remark 3. Thanks also go to Luchezar Avramov and Jim Shank for many helpful discussions.

## REFERENCES

- Beaumont, R. A., Peterson, R. P. (1955). Set-transitive permutation groups. *Canad. J. Math.* 7:35–42.
- Derksen, H., Kemper, G. (2002). Computational Invariant theory. *Encyclopedia Math. Sci.* 130 Springer.
- Fleischmann, P. (1998). A new degree bound for vector invariants of symmetric groups. *Trans. Amer. Math. Soc.* 350(4):1703–1712.
- Göbel, M. (1995). Computing bases for rings of permutation-invariant polynomials. *J. Symb. Comp.* 19:285–291.
- Neusel, M. D. (2007). Degree bounds—An invitation to postmodern invariant theory. *Topology Appl.* 154:792–814.
- Neusel, M. D., Smith, L. (2002). *Invariant Theory of Finite Groups*. Math. Surveys Monogr. Vol. 94. Amer. Math. Soc.
- Noether, E. (1926). *Der Endlichkeitssatz der Invarianten Endlicher Linearer Gruppen der Charakteristic  $p$* . Nachr. Ges. Wiss. Göttingen, pp. 28–35; Reprinted in: *Collected Papers*. Berlin, Springer-Verlag, 1983, pp. 485–492.
- Wehlau, D. L. (2006). The Noether number in invariant theory. *Comptes Rendus Math. Rep. Acad. Sci. Canada* 28(2):39–62.